DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

September 2008 Issue

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

DTI eSecurity News - Portable Device Security

What is at Risk?

Many of us, especially those who travel for business, rely on laptops and blackberries because they are small and easily transported.

Since these devices are so portable, extra precautions need to be taken to prevent their loss or theft. The data stored on the device is often far more valuable than the actual device itself.

Before You Leave the Office

Password-protect your portable devices
Use a strong password to login to your device and to protect access to your data.

Remove information that is not needed
Don't carry non-public data on your laptop, unless it is necessary to your work.

Always back up your files
To avoid losing and compromising information, be sure to back up your files and store them in a separate location.

Record identifying information and mark your devices
For recovery purposes, record the make, model, and serial number of your devices. Keep the information separate from your devices and in a safe place.

Have your laptop configured to boot from the hard-drive first
This prevents someone from rebooting your laptop from another drive; e.g. CD, flash drive.

Produced in part by US-CERT

What is a Strong Password?

It is recommended that a password is created with a minimum length of 12 characters, as it will become the minimum requirement for Homeland Security, NIST and others.

Passwords should contain characters from at least three (3) of the following four (4) classes:

- **English upper case letters (A, B, C......Z)**
- **English lower case letters (a, b, c......z)**
- **English (Arabic) numerals (0, 1, 2......9)**
- **English Non-alphanumeric (#, $, %......)**

Ideas When Traveling

Traveling by air, rail, or public transportation
Keep your portable devices with you in a carry-on bag. Never store your laptop or blackberry in checked luggage. Watch your devices carefully during screening processes. Never let a driver or baggage handler take your portable devices out of your view or leave them unattended.

Traveling by car
If it is necessary to leave a portable device in a car, lock it in the trunk or other location, where it will be out of sight. Never leave electronic devices in cars for extended periods, during hot or cold weather, or overnight. Never leave the vehicle unlocked when unattended.

In the hotel room
If a room safe is available, lock your devices in the safe. If they don't fit inside the safe, ask the hotel staff for the use of the hotel safe or other secured location.

At conferences and trade shows
Keep your portable devices with you. Never leave them unattended in your hotel room or in a conference room.

Downplay your portable devices
Store and carry your laptop in a non-descript bag, such as a shoulder bag or a briefcase. Carry smaller devices out of plain view.

Treat them like cash
Think of your laptop as $1,500 in cash, and protect it accordingly.

Report Loss or Theft IMMEDIATELY

In the event that your portable device is lost or stolen and it either contains business files or is owned by your employer, report it as soon as possible to the following:

- Local law enforcement agency
- Your organization's Security Office/IT Support Team/ Help Desk
- Hotel or conference staff
- Airport or other transportation staff

Be prepared to report the date and time the incident was detected, the nature of the incident, and identifying information about the device.

Questions or comments?
E-mail us at eSecurity@state.de.us

For more information on how to protect you, your family, and your computer, visit http://dti.delaware.gov/cybersecurity.